

office action. Applicants respectfully request withdrawal of the final rejection and request allowance of the pending claims.

The Final Office Action contains nearly identical language to the rejection in the previous office action. In the Final Office Action's response to Applicants' arguments section, the Office Action indicates that the references are properly combinable because "the added flexibility of keys with selectable expiration times as taught by Dolphin provides a reason to combine Dolphin and Lewis." This appears to be an over generalized interpretation of Dolphin and a conclusory statement. Applicants respectfully submit that Dolphin cannot be cited without consideration of what the Dolphin system is, and how the Dolphin invention carries out its disclosed process. Applicants again respectfully request a showing as to factual support for a teaching or motivation to combine a proper characterization of the teachings of the Lewis and Dolphin references in view of the Applicants claim language.

In addition, the Office Action indicates that the Examiner does not believe that the improvements that Lewis presents are used in the rejection of the present invention. The Examiner indicates that selective teachings of the Lewis reference are used primarily to merely teach a public key cryptosystem in which keys are replaced. Applicants respectfully submit that Lewis cannot be cited without consideration of how the Lewis invention carries out its disclosed process.

The Lewis reference is directed to a key replacement system in a public key cryptosystem. The Lewis system does not teach or suggest, inter alia, selectably varying key expiry data for digital signatures or encryption keys as claimed. In fact, Lewis is directed to a completely different problem. The Lewis reference is directed to securing replacement keys so that it is computationally difficult to determine a replacement key from its masked version. An active public key and a hash of a replacement public key is provided by a key server to nodes of the network. Each time a key request is performed, the active public key is discarded. A key replacement message is signed by an active private key and a replacement private key. Accordingly, the message is signed by a

replacement private key from an entity that knows the replacement private key before the message is sent.

Applicants respectfully submit that the Office Action fails to provide a showing as requested by Applicants, of a teaching or motivation to combine distinctly different aspects of distinctly different systems. Applicants respectfully note that obviousness cannot be established by combining the teachings of prior art by using hindsight reconstruction "to pick and choose among isolated disclosures in the prior art to deprecate the claimed invention." In re Fine, 5 U.S.P.Q. 2d 1596, 1600 (Fed.Cir. 1988). Moreover, the Office Action does not address the claim language set forth in the claims but instead overly generalizes the claimed invention in an attempt to render the claims obvious.

For example, Applicants claim, inter alia, a method and apparatus directed to digital signature keys and a method and apparatus directed to public key based encryption/decryption key pairs. For example, in claim 1, Applicants claim inter alia, a method for providing updated digital signature key pairs in a public key system by, providing, through multi-client manager unit, selectable digital signature expiry data including, for example, public verification key expiry data and selectable private signing key expiry data that are selectable on a per client basis wherein the digital signature key pairs are not shared among users. In addition, the selected public key expiry data and selected private key expiry data are stored for association with a new digital signature key pair. Other novel aspects are set forth in the dependent claims.

The Dolphin reference is directed to a system for access control for portable data storage media to facilitate, for example, secure periodic distribution of several different sets of information through the use of an access code. These decryption access codes are provided to users to allow users to gain access to distributed media. The Dolphin reference teaches one symmetric key for all users wherein different date ranges are associated with the same key depending upon the user. One encryption key is generated from a previous key. The Dolphin reference teaches that the access code or key may have expired for one user but the same key is still good for other users. Moreover, the

key expiration date apparently used in the Dolphin reference relates apparently only to a public key and is not related at all to decryption keys or private keys. Since only one key is used for all users, Dolphin does not provide the security required for a public key infrastructure system as claimed by Applicants. The Dolphin reference appears to be completely silent as to, inter alia, providing updated digital signature key pairs through a multi-client manager unit and providing selectable expiry data for digital signature keys, as implied in the Office Action.

Dolphin also teaches away from using public key pairs for encryption by using the same key for multiple users in contrast with Applicants' claimed invention. For example, Applicants claim, for example, inter alia, in Claim 9, a method for providing updated encryption key pairs in a public key system by providing selectable expiry data including public encryption key expiry data associated with a public encryption key, storing the selected public encryption key expiry data for association with a new encryption key pair and generating a new encryption key pair that is not computable from a previous encryption key pair, and associating the stored selected expiry data with the new encryption key pair to effect the transition from an old encryption key pair to a new encryption key pair.

When reviewing the claim language, the Dolphin reference is directed to a completely different system and is for access control for portable data storage media to facilitate, for example, secure periodic distribution of several different sets of information through the use of an access code. The symmetric key based operation of Dolphin would have to undergo extensive modification to be a public key based system. It is not understood how such a system would operate and the Office Action has not provided any facts to support how such a system must operate. For example, there appears to be no teaching, suggestion or motivation to substitute digital signature public key pairs for symmetric encryption techniques of Dolphin in any of the references or in any information provided in the Office Action. Moreover, public key-based systems have been around for decades and no other references to Applicants' knowledge teach or suggest the claimed invention as set forth by Applicants. In addition, there is no


indication in the references that there is a problem with the Dolphin method, the symmetric key type access control approach, to modify it to be completely different. Nor is there any motivation to modify the Lewis system, other than applicants own specification. Therefore, Applicants again respectfully request a showing as to the teachings, suggestion or motivation other than Applicants' own disclosure for the combining of the proper teachings of these references.

As to claim 3, 4, 6, 7, 8, 12, 16, 19 and other dependent claims, the Office action does not address limitations of these claims. For example (see claim 3), no teachings are cited relating to, inter alia, providing variable update privilege control on a per client basis to facilitate denial of updating the digital signature key pair on a per client basis.

Claims 5, 19 and 25 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Dolphin and Lewis as applied to claims 1, 14 and 25 and further in view of the Applicants' prior art. Applicants reassert the arguments made above and further respectfully note that conventional public key cryptographic systems typically have a fixed default period that is the same for all clients on the system. The fixed default period is generally a fixed percentage of a total key lifetime that is not adjustable by a manager or certification authority. Applicants claim, inter alia, initiating, by a client unit, digital signature key pair update requests based on whether difference between a current data and a digital signature private key lifetime end date is less than an absolute predetermined period of time, and based on whether the difference between a current date and the digital signature private key lifetime end data is less than a predetermined percentage of the total duration of a digital signature private key lifetime. No such digital signature key pair update request or basis for such a request is taught or suggested in any of the references or the prior art. It is Applicants' own disclosure which teaches such an invention which provides many advantages over conventional systems. Applicants respectfully request a teaching in the references of such a digital signature key pair update request and the basis for initiating such a request as claimed.

For the reasons stated above, Applicants request that the final rejection be withdrawn and that the claims be passed for allowance. The Examiner is invited to contact the undersigned attorney by telephone or facsimile if the Examiner believes that such a communication would advance the prosecution of the present patent application.

Respectfully Submitted,

By: 
Christopher J. Reckamp
Registration No. 34,414
Attorney for Applicants

Markison & Reckamp, P.C.
PO. Box 06229
Wacker Drive
Chicago, Illinois 60606-0229
Telephone: (312) 939-9800
Facsimile: (312) 939-9828